IN THE UNITED STATES DISTRICT COURT FOR
THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

| | | |
|---|---|---|
| **SILVERPOP SYSTEMS, INC.,** | ) | |
| | ) | |
| **Plaintiff,** | ) | |
| | ) | |
| **v.** | ) | **Civil Action File** |
| | ) | **No. 1:12-CV-2513-SCJ** |
| **LEADING MARKET TECHNOLOGIES, INC.,** | ) | |
| | ) | |
| **Defendant.** | ) | |

**SILVERPOP SYSTEMS, INC.'S MEMORANDUM IN SUPPORT OF MOTION FOR SUMMARY JUDGMENT**

**TROUTMAN SANDERS LLP**

John P. Hutchins
Georgia Bar No. 380692
*john.hutchins@troutmansanders.com*
Courtney E. Ferrell
Georgia Bar No. 575948
*courtney.ferrell@troutmansanders.com*
Benjamin W. Cheesbro
Georgia Bar No. 648368
*benjamin.cheesbro@troutmansanders.com*

For Plaintiff Silverpop Systems, Inc.

5200 Bank of America Plaza
600 Peachtree Street, N.E.
Atlanta, GA 30308-2216
Telephone: (404) 885-3000
Facsimile: (404) 885-3900

Defendant Leading Market Technologies, Inc. ("LMT") counterclaims for breach of contract, fraud and negligence, arising out of a 2010 Data Breach. LMT claims that the value of the email addresses it stored in Silverpop's technology system was destroyed by the Breach. Silverpop moves for summary judgment. LMT has not suffered the damages it claims, nor is its proof of damages sufficient. Further, damages it claims are consequential and, therefore, not recoverable. Its claims also fail because it cannot show a causal connection between the Breach and any damages, establish the elements of its tort claims, or overcome the legal bar to those claims.

## FACTS

The facts relevant to Silverpop's Motion are all set forth in Silverpop's Statement of Material Facts as to Which There is No Genuine Issue to Be Tried ("Statement of Facts" or "SOF"), which is incorporated herein by reference.

## ARGUMENT AND CITATION OF AUTHORITIES

### I. Legal Standard

The Court is well-aware of the summary judgment standard as stated Federal Rule of Civil Procedure 56(c) and the burden-shifting required under *Celotex*[1] and *Hickson.*[2] Silverpop will not repeat those well-known standards here.

---

[1] 477 U.S. 317, 323 (1986).
[2] 357 F.3d 1256, 1260 (11th Cir. 2004).

## II. Summary judgment is warranted as to all three of LMT's claims.

Summary judgment on all of three of LMT's claims is warranted. First, the value of LMT's MarketBrowser email list has not been reduced to zero, as LMT claims. Second, LMT cannot establish a causal connection between the Data Breach and the facts that it claims caused its damages. Third, LMT's claimed damages are consequential and barred by the parties' contract. Fourth, LMT failed to seek rescission, barring its fraud claim. Fifth, LMT cannot establish any actionable misrepresentations. Sixth, LMT's negligence claim is barred by the economic loss rule. Lastly, LMT cannot establish a duty giving rise to negligence.

### A. LMT Cannot Prove Its Damages.

LMT must show damages.[3] It cannot. The value of LMT's email list ("MB List") has not been reduced to zero, as LMT claims, and LMT cannot establish a causal connection between the Breach and the facts that caused its damages.

#### 1. It is undisputed that the email list's value has not been reduced to zero.

LMT claims that the value of its MB List as a "saleable asset" was reduced from whatever pre-Data Breach value it had to worthless afterwards.[4] It offers two

[3] *United States ex rel. Friddle v. Taylor, Bean & Whitaker Mortgage Corp.*, 2012 U.S. Dist. LEXIS 42473 (N.D. Ga. Mar. 27, 2012) (breach of contract); *Alexander v. A. Atlanta Autosave, Inc.*, 272 Ga. App. 73, 76 (2005) (negligence); *Remax N. Atlanta v. Clark*, 244 Ga. App. 890, 893 (2000) (fraud).

[4] LMT Initial Disclosures (Third Amended), at 11-12, and ¶8.

approaches for its pre-Breach valuations: (1) "replacement cost"[5] and, (2) an income valuation for LMT email line of business.[6] The difference between the pre-Breach valuations and zero is LMT's claimed loss. LMT's post-Breach value of zero rests on the opinion of Marc Prosser. But the alleged worthless value is belied by LMT's actual post-Breach commercial use, and Prosser's opinion depends on two premises LMT cannot prove: (1) the necessity of disclosing the Breach to any potential buyer as part of any sale involving the MB List and, (2) that no reasonable buyer would purchase the list after disclosure.

**a. *LMT admitted that the list still has value.***

The source of the email addresses loaded into Silverpop's Engage system by LMT was LMT's eMaster database.[7] LMT admits that it still has access to all of those email addresses. It does not believe those email addresses have become unusable, just less valuable. LMT continues to use the email addresses exactly as before the Breach – sending stock-related advertisements. It continues to generate revenue from this business. It also uses the MB List in bartering arrangements, in which it trades access to its list in exchange for access to lists owned by others. It has made no changes

[5] *Id.*; Deposition of Jay Kemp Smith, Individually, and of Leading Market Technologies, Inc., Pursuant to Rule 30(b)(6), 371:11-22.
[6] Deposition of James F. Dondero, Ex. 7, Expert Report, at 3-4, and attachments C&D.
[7] SOF ¶¶ 12-19; 63-64.

whatever in the procedures that it uses to identify "usable" email addresses stored in its eMaster database. LMT's MarketBrowser product continues to attract new registered users, and the eMaster database continues to grow, now including approximately 1.5 million email addresses. LMT cannot distinguish addresses that were allegedly compromised from those that were not. It uses its database exactly as it did before, without regard to the Breach.[8]

Notwithstanding, LMT's damages claim is based 100% on the premise that the list has no value after the breach. Its principals (Jay Smith and Steve Clark) offer self-serving opinions that the list no longer has value as an asset, but their continued use of the list belies the veracity of those opinions. LMT offers the opinion of Marc Prosser that the list has no value.[9] But Prosser failed to even make inquiry regarding LMT's continued use of the list. His opinion cannot overcome the fact that the list obviously still has value, which completely undercuts LMT's damages claim.

**b.** ***LMT cannot prove necessity of the Breach's disclosure in a sale or that no reasonable buyer would purchase the list after learning of the breach.***

LMT offers no credible evidence that the Breach must be disclosed in the event it wants to sell the list. It cannot point to any pre- or post-Breach negotiations

[8] SOF, ¶¶ 69-78.
[9] Prosser's entire opinion should be excluded; a *Daubert* motion will follow.

regarding a sale of the MB List where such disclosures were requested.[10] Again, it offers the opinions of its principals, but these opinions have no basis in fact or law. Clark testified that his opinion is based merely on his "upbringing" and "common sense."[11] Smith testified he did not know why disclosure would be required:

Q. Do you know why the disclosure of the hacking incident would be a necessary step in selling of the list?

A. I would consider that a fraud or omission to not tell a buyer that, I guess. I don't know. It seems like you have to tell somebody that. They would be pretty upset if they learned about it.[12]

When asked whether the disclosure requirement would remain forever, Smith said, "One would have to talk to counsel about what are the duties of disclosure."[13]

LMT's own conduct contradicts its position. It is currently selling and bartering access to its list without disclosing the Breach to its advertising customers or trading partners. It has never made any notification under any of the state data breach notification statutes, and it has not otherwise notified its customers who are currently paying or trading for access to the List.[14]

LMT offers Prosser's opinion that disclosure would be required, based on "business ethics," but he could not establish any particular expertise in the field of

[10] SOF, ¶ 81-82.
[11] Deposition of Leading Market Technologies, Inc., designee Steven Clark Pursuant to Rule 30(b)(6) 225:3-7.
[12] LMT/Smith Dep., 379:17-24.
[13] LMT/Smith Dep., 380:5-6.
[14] SOF, ¶¶72-77.

"business ethics" or point to any recognized ethical code or standard as support for his opinion. Prosser was completely unaware of whether LMT is still selling access to the List, so he was unaware of the hypocrisy of LMT's nondisclosure.

Further, LMT has offered no admissible, credible evidence that no reasonable buyer would purchase the list as an asset, with knowledge of the Breach. Certainly, the list has commercial value, which LMT is still exploiting. As a list with commercial value, there is some price the list would fetch if it were offered for sale. But LMT has not tried to sell it. Its claim that no reasonable buyer would pay any price for the list is merely an assumption. LMT offers only Prosser's opinion on this topic, but LMT's post-Breach commercial use of the MB List refutes his opinion.

There is no genuine issue as to whether the value of the MB List has been reduced to zero. Plainly, it has not. LMT's damages claim regarding all three counts of its counterclaims is based, in its entirety, on this premise. Since LMT cannot prove the premise, its entire damages claim fails, and Silverpop is entitled to summary judgment as to all counts.

**2. LMT cannot establish a causal connection between the Breach and the facts that it claims ultimately caused its alleged damages.**

LMT must show that Silverpop's conduct caused the damages it claims.[15] Steven Clark, LMT's principal, testified that, in addition to the "no reasonable buyer" theory debunked above, the "effectiveness and rentability" of the MB List has been diminished, making it less valuable.[16] But LMT cannot establish a causal connection between the Breach and the causes it speculates have diminished the list's value.

The Breach was discovered by Silverpop on approximately November 23, 2010. LMT claims that it began to experience a drop-off in revenue from its MarketBrowser business in mid-2011. But as to how a data breach could be connected to a drop-off in revenue seven months later, LMT only speculates:

Q. The effectiveness of the list and its rentability. Tell me why that value has gone down.

A. I have to speculate to some extent because what I'm working from is the evidence that its value has gone down because the sales of the list plummeted and the size shrank.

---

[15] *Alexander v. A. Atlanta Autosave, Inc.*, 272 Ga. App. 73, 76 (2005) ("In the analysis of a negligence action, the plaintiff must . . . show a duty, a breach of that duty, causation, and damages."); *United States ex rel. Friddle v. Taylor, Bean & Whitaker Mortgage Corp.*, 2012 U.S. Dist. LEXIS 42473 (N.D. Ga. Mar. 27, 2012) ("the elements of a breach of contract action are (1) a valid contract, (2) breach of that contract, and (3) damage caused by the breach."); *JTH Tax, Inc. v. Flowers*, 302 Ga. App. 719, 723 (2010) ("To establish a cause of action for fraud, a plaintiff must show that actual damages, not simply nominal damages, flowed from the fraud alleged.").

[16] LMT/Clark Dep., 224:9-18.

. . .

Q. When you say the sales of the list plummeted, is that another way of saying . . . that the revenue of that business line declined?

A. That's correct.

Q. And is the reason that your revenue from the business line declined because your advertising customers made fewer requests for . . . use of that particular list.

A. Yes.

Q. And do you attribute the fewer requests for that particular list to be used to something having to do with Silverpop's data breach?

A. Yes.

Q. How are they related?[17]

At this point, Clark launched into speculation and circular reasoning about what might have happened to the email addresses. He speculated that "the people who stole the list would begin sending unauthorized spam e-mail themselves cause people to reject or silently discard or report basically cause various kinds of erosion of our list. And we certainly saw a precipitous erosion of the list."[18] He opined that the reason LMT saw fewer requests by customers for use of the MB List is that "the effectiveness of advertising using that list has declined."[19] He concluded that the decline in effectiveness is tied to the Breach because, as he said, "I don't think that there are any other factors that could explain both the timing and the size of this

[17] LMT/Clark Dep., 225:11-17; 230:19.
[18] LMT/Clark Dep., 230:25-231:10.
[19] LMT/Clark Dep., 232:19-24.

phenomenal shift."[20] When asked what other factors he analyzed, he cited the decline in revenues and orders.[21] Thus, in a dizzying display of circular logic, Clark assumes the decline in effectiveness based on the decline in revenue and orders. The only particular fact that Clark points to as indicating that the Breach and revenue decline are linked is timing – "there was a breach in October, November . . . 2010 . . . and by mid-2011 our revenues started plummeting."[22] When asked if he had any reason to believe that the version of the MB List stored in Silverpop's system was "being used by bad guys," he responded again with the revenue decline (and "efficacy" of the advertising, which has already been shown he assumes from the decreased revenue).[23] When asked to explain why he concludes that the drop-off in revenue was the result of "bad guys" using the MB List, he responded, "I came to that conclusion by the elimination of other possibilities to explain an otherwise inexplicable statistical anomaly.[24] When asked what he believes "the bad guys" could have done with the MB List that would cause the revenue decline, he once again speculated: "delivery of malicious payloads and take over other people's machines," "spamming," a "pump-and-dump scam," identity theft of persons on the MB List and "phishing" attacks on

[20] LMT/Clark Dep., 233:4-8.
[21] LMT/Clark Dep., 232:25-233:20.
[22] LMT/Clark Dep., 235:11-14.
[23] LMT/Clark Dep., 236:12-22.
[24] LMT/Clark Dep., 238:13-20.

those users.[25] When asked for evidence that these schemes have been actually carried out by the hackers, he responded, "I don't have actual knowledge of anyone using LMT's names [the MB List] for these purposes."

The cause of what LMT claims diminished "effectiveness and rentability" of the MB List is malicious use by the Data Breach hackers of the MB List, leading to MarketBrowser registered users opt-outing of advertisements sent by LMT, or to ISPs identifying emails appearing to come from LMT as potentially malicious. That leads to a less effective advertising, and customers notice take their advertising dollars elsewhere.

But the only fact that LMT posits in support of this causal connection is the timing of its decline in revenue. There is no evidence that:

- Since November 2010, LMT has experienced a higher "opt-out- rate"[26]
- ISPs have blocked emails purportedly originating from LMT (or Silverpop)
- Any user on LMT's MB List experienced a "phishing" or identity theft
- Even one email purportedly originating from LMT that contained a malicious payload
- Anyone on the MB List reported higher spamming rates.

[25] LMT/Clark Dep., 238:24-241:4.
[26] LMT/Clark Dep., 245:10-13.

All LMT has is timing. The Eleventh Circuit recently held that timing is insufficient to sustain a claim that a data breach led to specific harm.[27]

LMT cannot establish a causal connection between the Breach and the speculative facts about hacker misconduct that it claims ultimately caused the diminished value of the MB List. Thus, summary judgment is proper.

**B. <u>The Breach of Contract Claim is Barred by the Contract</u>.**

The damages LMT seeks are classic consequential damages, and thus barred by the Paragraph 10.1 of the parties' contract.[28]

Direct damages "arise naturally [from the breach] and according to the usual course of things" the parties contemplated when the contract was made.[29] They are necessarily inherent in the contract and represent the benefit of the bargain.[30] "Remote or consequential damages are…independent of any collateral enterprise entered into in

---

[27] *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1326 (11th Cir. Fla. 2012) (holding that "mere temporal connection is not sufficient" to survive a motion to dismiss; plaintiff must plead "allegations of a nexus between the two instances beyond time and sequence."). *Kahle v. Litton Loan Servicing LP*, 486 F. Supp. 2d 705, 712 (S.D. Ohio 2007) (summary judgment on plaintiff's negligence claim where plaintiff "admitted, that to her knowledge, no unauthorized use of her personal information has occurred.").

[28] SOF, ¶22.

[29] O.C.G.A. § 13-6-2 (2007).

[30] *Imaging Sys. Int'l*, 227 Ga. App. at 643-44 (observing that direct damages include damages which are "necessarily inherent in the contract" and "represent the benefit of the bargain"). *See also Acuity Brands, Inc. v. Thomas & Betts Corp.*, 2006 U.S. Dist. LEXIS 100590 (N.D. Ga. July 21, 2006) (citing *Imaging Sys. Int'l, Inc. v, Magnetic Resonance Plus, Inc.*, 227 Ga. App. 641, 643-44 (1997)).

contemplation of the contract…" and are typically defined as the loss of business opportunities, profits, and goodwill.[31]

LMT's claim is one diminution in value, or for lost profits (or lost revenues). Although LMT attempts to avoid the consequential damages waiver by characterizing the MB List as a "saleable asset," as if its claim is more akin to a property claim, its actual claim is for diminished value of the list. Clark admitted that the "asset value" of the email addresses at issue derives from the fact that they can be used.[32] Clark stated quite plainly that the email addresses in the MB List are not unusable. "No, they are not unusable. We use them to this day."[33] Rather, LMT's claim is simply that the MB List "became less valuable to [LMT] for email marketing purposes."[34]

LMT's claim may also be seen as a claim for lost profits, as LMT has admitted that "the sale of the database and MarketBrowser's product represents Leading Market's only opportunity in retrieving profit from its investment in MarketBrowser."[35] Or, as Clark has stated it, LMT claims that the Breach caused its

[31] O.C.G.A. § 13-6-8; *Imaging Sys. Int'l, Inc. v, Magnetic Resonance Plus, Inc.*, 227 Ga. App. 641, 643-44 (1997).
[32] LMT/Clark Dep., 166:4-18.
[33] LMT/Clark Dep., 223:16-24.
[34] LMT/Clark Dep., 133:18-23.
[35] LMT/Clark Dep., Ex. 93, p. 2; LMT Initial Disclosures (Third Amended), ¶8.

sales to plummet.[36] Plummeting sales leads to a decline in revenue, which leads to reduced profit.

No matter, LMT claims only consequential damages. Although there is no Georgia authority directly on point as to whether a diminution in value claim is a claim for consequential or direct damages, other states directly addressing the issue have held that diminution in value claims are for consequential damages.[37] In fact, in very similar case, *Allen Bros. v. Abacus Direct Corp.,*[38] a plaintiff sought damages for diminution in value of its customer list arising from the defendant's unauthorized renting and selling plaintiff's customer list, which was being stored by defendant.[39] The *Allen* court granted defendant's motion to dismiss, which argued that the plaintiff's claim was for diminution of value and therefore barred by the consequential damages waiver in the parties' agreement.[40] The court held that "it is clear that there are no allegations which support the inference that [plaintiff's] customer lists have some sort of independent and intrinsic value apart from their ability to provide a business advantage….The court has already held that loss of the

[36] *Supra* p. 7-9.
[37] *See Wyoming Sawmills, Inc. v. Transportation Insurance Co.*, 578 P.2d 1256 (Or. 1978); *Civic Ctr. Drive Apts. Ltd. P'ship. v. Southwestern Bell Video Services*, 295 F. Supp. 2d 1091 (N.D. Cal. 2003).
[38] *Allen Bros. v. Abacus Direct Corp.*, 2003 U.S. Dist. LEXIS 27751 (N.D. Ill. May 13, 2003).
[39] *Id.* at *5.
[40] *Id.* at *6.

ability to pursue a business advantage is a type of consequential damage that is barred by the contract."[41] Other courts have held that similar claims of diminution of business value or advantage are claims for consequential damages.[42]

Lost profits that do not arise directly out of the failure to perform the contract are also considered consequential damages, as is a claim based on lost customers. A claim for lost profits involving lost customers or inability to perform future services for customers constitutes indirect damages.[43] Moreover, "the loss of other business opportunities, other profits and good will falls squarely within the meaning of consequential losses."[44] LMT's claim, with regard to the "asset value" of this MB List, is that a major factor is that LMT enjoyed a "trust relationship" with the recipient.[45] Loss of that "trust relationship" is the same as loss of "good will." *Black's Law Dictionary* defines "good will" as "[a] business's reputation, patronage, and other intangible assets that are considered when appraising the business"[46]

---

[41] *Id.*
[42] *See, e.g., True N. Composites, L.L.C. v. Trinity Indus.*, 65 Fed. Appx. 266, 273 (Fed. Cir. 2003); *Ada Liss Group v. Sara Lee Corp.*, 2009 U.S. Dist. LEXIS 91792 (M.D.N.C. Sept. 30, 2009).
[43] *Imaging Sys. Int'l v. Magnetic Resonance Plus*, 227 Ga. App. 641, 644 (1997) (holding that damages for "what the user of the MRI would lose if the machine were not working and he was unable to perform diagnostic services for several patients" constitute indirect or consequential damages).
[44] Imaging Sys. Int'l v. Magnetic Resonance Plus, 227 Ga. App. at 644.
[45] LMT/Clark Dep., 166:16-167:3.
[46] Black's Law Dictionary 763 (9th ed. 2009).

Georgia courts have defined the phrase similarly.[47] The lost opportunity to extract the profits from its investment in MarketBrowser by selling the MB List or the MarketBrowser business to a third party, even if LMT could establish that lost opportunity as a fact, is clearly within the *Magnetic Resonance* court's meaning in defining consequential damages as "the loss of other business opportunities [or other profits]."[48]

In sum, the parties' contract bars any claim for consequential damages, and Silverpop is entitled to judgment as a matter of law on the breach of contract claim.

### C. LMT's Fraud Claim Is Barred by a Merger Clause, and LMT Cannot Prove that Silverpop Made False Representations.

LMT claims that Silverpop misled it into entering the Engage contract by falsely representing its security. But the parties' contract contains a merger clause which waived and disclaimed all representations not contained in the contract. In any event, the alleged false representations identified by LMT were general expressions of opinion, representations as to quality, or mere puffery, which cannot give rise to a fraud claim, or LMT cannot prove the statements were false when made.

---

[47] *See United Seal & Rubber Co. v. Bunting*, 248 Ga. 814, 817 (Ga. 1982) ("favor which the management of a business wins from the public, and the probability that old customers will continue their patronage and resort to the old place . . . .")

[48] *Imaging Sys. Int'l v. Magnetic Resonance Plus*, 227 Ga. App. at 644.

**1. The merger clause contained in the contract bars any fraud claim based on representations made before the execution of the contract.**

In support of the fraud claim, LMT alleges:

> Before entering into a contract to retain Silverpop's services and turn over its confidential list and other confidential information in 2005, the Plaintiff received written and oral assurances from Silverpop's employees that Silverpop had purchased state-of-the-art technologies and taken all of the necessary steps to ensure that its system could not be hacked into.[49]

However, the contract's merger clause (para. 9) disclaims any representations that may have been made in the time leading up to the execution of the contract.[50]

Where a contracting party claims that it has been fraudulently induced to enter a contract, that party has two options: (1) it may rescind the contract and sue for fraud; or, (2) it may affirm the contract and sue for enforcement of the contract.[51] If it elects to affirm and that contract contains a merger clause, that party cannot claim fraud but is instead "relegated to a recovery in contract . . . ."[52]

LMT did not rescind. Rather, it affirmed and continued to utilize Engage by sending 16 million emails to its MB List over several months after the Breach.

> Where a party who is entitled to rescind a contract on ground of fraud or false representations, and who has full knowledge of the material

---

[49] Leading Market Technologies, Inc.'s Answer And Counterclaims [ECF No. 4], ¶ 4 of Counterclaim, at 9.
[50] SOF, ¶21.
[51] *Brock v. King*, 279 Ga. App. 335, 340 (2006).
[52] *Id. See also Novare Group, Inc. v. Sarif*, 290 Ga. 186, 190 (2011); *Markowitz v. Wieland*, 243 Ga. App. 151, 153 (2000).

> circumstances of the case, freely and advisedly does anything which amounts to a recognition of the transaction, or acts in a manner inconsistent with a repudiation of the contract, such conduct amounts to acquiescence . . . . If a party to a contract seeks to avoid it on the ground of fraud or mistake, he must, upon discovery of the facts, at once announce his purpose and adhere to it. Otherwise he can not avoid or rescind such contract.[53]

Where there is no evidence of rescission, summary judgment in the opposing party's favor is proper.[54] LMT cannot show attempted rescission. At no point since the Breach has LMT made any statement to Silverpop that it was rescinding, nor does it seek rescission in this action. Continued use of Silverpop's Engage product for months after the Breach is "inconsistent with repudiation of the contract."

Even if LMT claims that it attempted to rescind the contract, the fraud claim still fails as a matter of law because, in its Complaint, LMT only seeks monetary damages, not rescission of the contract. Georgia law is clear that, even where a party claims that it "attempted rescission" before filing suit, if it fails to plead rescission, it is deemed to have affirmed the contract, and a fraud claim fails as a matter of law.[55]

---

[53] *Owens v. Union City Chrysler-Plymouth*, 210 Ga. App. 378, 380 (1993) (emphasis added) (holding fraudulent inducement claim failed where plaintiff continued to use a vehicle after discovery of fraud, despite the fact that plaintiff inquired about rescinding the contract) (citing *Gibson v. Alford*, 161 Ga. 672, 673 (1926)).

[54] *UWork.com, Inc. v. Paragon Techs., Inc.*, Nos. A12A2448, A12A2449, 2013 Ga. App. LEXIS 355, at *21-22 (Ga. Ct. App. 2013) (summary judgment on fraud claim over technology services contract, where claiming party never attempted rescission)

[55] *Markowitz v. Wieland*, 243 Ga. App. 151, 153 (2000) (Plaintiffs sought only money damages and failed to seek rescission in their complaint).

**2. The representations claimed by LMT were not specific enough to give rise to a fraud claim, or were not false when made.**

LMT's fraud claim also fails because the alleged misrepresentations LMT claims[56] are not sufficiently definite, and LMT cannot prove that they are false when made. A fraud claim can only be based on statements which are "empirically verifiable."[57] General expressions of opinion are not actionable,[58] nor are expressions of general quality.[59] Generalized boasts as to expertise are "puffery."[60]

Steve Clark claims that Silverpop represented it had "trust relationships" with ISPs that were built on competencies, practices and technologies that were agreed upon between Silverpop and the ISPs.[61] LMT has no evidence that this representation was false when made. Clark admitted that, to his understanding, Silverpop had the trust relationships that it claimed.[62] Clark points to Silverpop alleged statement that, to maintain these "trust relationships," it needed to "maintain the highest standards of

---

[56] SOF, ¶¶23-25.
[57] *Botes v. Weintraub*, 2010 U.S. Dist. LEXIS 22793, 23-24 (N.D. Ga. Mar. 11, 2010)(citing *Next Century Communs. Corp. v. Ellis*, 171 F. Supp. 2d 1374, 1379-80 (N.D. Ga. 2001)).
[58] *Id.*
[59] *U-Haul Co. of Western Georgia v. Dillard Paper Co.*, 169 Ga. App. 280, 281 (1983).
[60] *See FieldTurf USA Inc. v. TenCate Thiolon Middle E., LLC*, 2013 U.S. Dist. LEXIS 66837 (N.D. Ga. May 10, 2013).
[61] SOF, ¶23(a).
[62] SOF, ¶26.

security and security practices and security technologies. . . ."[63] But Clark does not claim this as false. Again, he believes Silverpop had the trust relationships it claimed. In any event, a representation that Silverpop maintained "the highest standards" is not empirically verifiable.

Clark claims that Silverpop represented that "We do all of these things well," which he took to mean that Silverpop had "authentication protocols, log-in procedures . . . [a]ccess control protocols . . . IP identification protocols . . . [h]ardware firewalls."[64] "We do all of these things well" is plainly an opinion of general quality. In any event, Silverpop had the security measures.

As Clark defines it,[65] Silverpop had "access control."[66] Clark admits he has no reason to think otherwise. Rather, he believes the access controls were deficient.[67]

Clark offered a definition of " state-of-the-art authentication services" to include "a log-in identifier, an account name unique to LMT; a user name or an operator name, a way to identify who was doing what; and reasonably secure

[63] SOF, ¶23(b).
[64] SOF, ¶23(c).
[65] SOF, ¶27.
[66] SOF, ¶¶28-34.
[67] LMT/Clark Dep., 27:13-29:21.

password requirements . . . all taking place under SSL . . . ."[68] Silverpop employed all of these features in 2004 and continuing through 2010, including SSL.[69]

With regard to "IP identification protocols," Clark merely described the very trust relationships which he admitted Silverpop had.

> "In part of the general description of the trust relationship between Silverpop and ISP's, there is a great deal of importance about IP addresses – internet protocol addresses. And I remember hearing a description of how [the ISPs, Hotmail for example] keep very carefully controlled list[] of which addresses belong to which mail originators." . . . "the Silverpop and the Hotmails stay in communication about this, and that's part of an overarching architecture of very carefully controlled IP addresses for mailing, for client log-in, for access to various services . . . there is an architecture in a sense to IP addresses. Some of which . . . are identifiable as belonging to Silverpop specifically. In other words, IP addresses are a Silverpop-identifiable property."[70]

In large part, Clark understood Silverpop's description of this issue correctly, except as it relates to client log-in and access to services.[71] "Controlled IP addresses" has nothing to do with customer log-in to Engage.[72] It relates to (and in 2004 would have related to) emails sent <u>out</u> from Engage.[73] Those emails originate from the "controlled IP addresses," which increases the likelihood that they will be delivered to the desired

---

[68] LMT/Clark Dep., 275:10-276:25.
[69] SOF, ¶¶30-31, 35-36.
[70] LMT/Clark Dep., 35:5-36:12.
[71] Declaration of Kelly Thompson ¶4.
[72] Thompson Dec., ¶9.
[73] SOF, ¶37.

recipient.[74] This is the value proposition that Silverpop offers, and it is a main reason why customers like LMT use Silverpop's services instead of simply sending the emails from their own systems.[75] Clark's testimony, including why he believes Silverpop's representation about this issue was false in 2004, does not even make sense.[76] He claims that "that the IP address from which [LMT's] list was stolen was in Amsterdam in the Netherlands, which gives lie to the notion that they were controlled to within Silverpop IP addresses."[77] But Engage is an Internet-based service, meaning ALL clients log-in over the Internet.[78] Clark could have logged from the Netherlands. He does not claim that Silverpop ever represented that *user access* to Engage over the Internet (by LMT or anyone else) would be limited to only certain IP addresses owned by Silverpop. The IP addresses from which customers log-in to Engage are IP addresses owned and controlled by the customer, not by Silverpop.[79] If it were not so, customers like LMT could not gain access to Engage from IP addresses belonging to the customer, which is the whole point of an Internet-based service.

---

[74] SOF, ¶¶ 37-42.
[75] Thompson Dec., ¶8.
[76] Thompson Dec., ¶9.
[77] LMT/Clark Dep., 36:13-21.
[78] Thompson Dec., ¶3; SOF ¶43.
[79] SOF, ¶44.

Nonetheless, if LMT had desired that its access to services be limited to a certain set of identified IP addresses *owned by* LMT, Silverpop could have configured obliged.[80] But LMT never requested that.[81] It never provided Silverpop with a list of specific IP addresses that would be the total universe of IP addresses from which LMT could access Engage.[82] Clark even admitted that he did not expect Silverpop to know the IP addresses of LMTs authorized computers.[83]

Regarding "firewalls,"[84] Silverpop had hardware firewalls in place in 2004.[85]

With regard to what Clark terms Silverpop's "training culture,"[86] Clark claims that Silverpop "represented that part of what [Silverpop does] is stay up on the latest of threats, responses, defenses so that they can protect themselves, you know, stay on the cutting edge of protecting themselves against intrusion, bad guys. Everything. And that's part of that culture."[87] Clark's belief that this "training culture" did not exist rests merely on the fact that the Breach occurred.[88] But, Silverpop did train its employees to be aware of the risks involved in its industry, including Phishing

[80] SOF, ¶45.
[81] SOF, ¶46.
[82] SOF, ¶47.
[83] SOF, ¶48.
[84] SOF, ¶23(c).
[85] SOF, ¶¶49-52.
[86] SOF, ¶23(d).
[87] LMT/Clark Dep., 30:9-10; 37:16-38:3.
[88] LMT/Clark Dep., 38:4-18.

attacks.[89] Even so, the statements cited by Clark on this issue – a training "culture," "stay up on," "stay on the cutting edge" are not empirically verifiable statements. They are sales "puffery" at the most. The same is true with regard to Clark's claims about Silverpop's alleged representations that "We're on top of this. We stay with it."[90] These statements are not actionable.

Clark also stated that Silverpop represented that it would "monitor and scrub for malware"[91] but again there is no evidence that this statement was false. Silverpop did monitor for and attempt to protect against malware.[92] Other the Breach itself, LMTs points to no evidence that Silverpop did not.

As far written assurances,[93] most of statements identified by LMT are not empirically verifiable, nor were they false when made. Exhibit 29's claim that Silverpop used "state-of-the-art" security technologies is not empirically verifiable—it is an opinion, a general statement of quality, and sales puffery. Clark defined "state-of-the-art" as "represent[ing] the best practices available to a practitioner at the time."[94] This is not a concrete definition capable of being quantified. "Best practices" is merely a general opinion of quality. Clark opined that "state-of-the-art" is a "commonplace

[89] SOF, ¶53.
[90] SOF, ¶23(d).
[91] SOF, ¶23(f).
[92] SOF, ¶¶33, 50, 53 & 59.
[93] SOF, ¶¶24-25.
[94] LMT/Clark Dep., 67:14-21.

expression," yet he admitted when asked to define the term, he made up his definition on the spot.[95]

Exhibit 29 includes two of the same terms already discussed above – "access control" and "authentication." Similarly, Clark stated with regard to "data integrity and encryption" that he "expected SSL to be in place … [and] also would have expected that there would be encryption of data such that … if you didn't have authority to access [a file], you couldn't get at them by simply having authority over the system."[96] He admitted that really just describing another type of "access control"[97] which was in place in 2004. SSL was also available in 2004.

With regard to "audit control," Clark stated that he expected "Silverpop would keep logs of every activity that took place so that actions could be reconstructed,"[98] but he never claimed that Silverpop explained "audit control" in this way. Clark does not believe that Silverpop lacked audit control in 2004, but believes it was deficient.[99] In fact, Silverpop employed many audit controls.[100]

No terms on Exhibit 29 are more amorphous that "system security" and "network security." These generic terms are not empirically verifiable. Clark took

[95] LMT/Clark Dep., 69:6-16.
[96] LMT/Clark Dep., 283:10-284:21.
[97] LMT/Clark Dep., 284:2-20.
[98] LMT/Clark Dep., 285:11-18.
[99] LMT/Clark Dep., 75:23-76:3.
[100] SOF, ¶¶54-56.

"system security" to mean that Silverpop would have “security features inherent in the operating system environment . . . of the machines themselves separate from the Engage product”[101] which he explained as “network security, correct employment of features inherent in the computer operating systems themselves, best practices in the administration of machines, and password and access.”[102] Even Clark says that the difference between “system security” and “network security “ is “splitting hairs,” but that it would include “things like firewalls, either hardware or software firewalls. Limited IP address access [and] tight control over what locations are allowed to access what systems and services.”[103] As should be plain by now, however, these two generic terms could mean any number of security controls at the system or network level, dozens of which Silverpop had. Moreover, in addition to all the security protections already mentioned, Silverpop employed a practice of "hardening" its systems and also had a security operations center in which IBM was hired to watch “for anomaly type traffic, things that looked like intrusion . . . traffic.”[104] However one defines "system security" or “network security," Silverpop clearly had it.

[101] LMT/Clark Dep., 285:19-286:3.
[102] LMT/Clark Dep., 286:4-16.
[103] LMT/Clark Dep., 287:3-25.
[104] SOF, ¶¶57-58.

With regard to Exhibit 25, Clark interpreted this Exhibit to relate exclusively to security,[105] though it is obvious that this is not the purpose of this marketing tool. The description of Silverpop's security is on a completely different part of the webpage, shown in Exhibit 29. The representations Clark points to on Exhibit 25 are "sales talk" representations of general knowledge and quality.

Clark admits Silverpop had the "knowledge of the full range of issues" referenced on Exhibit 25.[106] Regarding "risk sensitivity," Clark reads more into Exhibit 25 than the text suggests. The Exhibit actually states, "from quality assurance to list scrubbing and opt-out capabilities, we are sensitive to the power and inherent risks of email, and we eliminate those risks". The statement itself does not mention security at all. It relates to the risk of email marketing, like violating CAN-SPAM by not honoring opt-outs or removing dead email address.[107] Security is covered on Exhibit 29. Not surprisingly, LMT admits that, with regard to its own eMaster database, it keeps dead emails forever.[108] Silverpop's opt-out capabilities, list scrubbing and quality assurance is part of the "value-added" that Silverpop offers to customers,[109] which is what is described in this paragraph.

---

[105] LMT/Clark Dep., 88:3-21.
[106] *Id.*
[107] Declaration of Thomas William Alvey, III, ¶¶16-19.
[108] LMT/Clark Dep., 119:8-15.
[109] Alvey Dec., ¶19.

The remainder of the items identified on Exhibit 25clearly puffery, general statements of quality and not empirically verifiable. Like the rest of the statements on Exhibit 25, they do not even mention security, even arguably.

## D. Silverpop is Entitled to Summary Judgment on LMT's Negligence Claim Because LMT Cannot Overcome the Economic Loss Rule or Prove a Duty.

LMT's purely economic loss bars a negligence claim. Further, LMT cannot establish a duty sufficient to establish negligence.

### 1. LMT's negligence claim is barred by the economic loss rule.

The economic loss rule "generally provides that a contracting party who suffers purely economic losses must seek his remedy in contract and not in tort."[110] The rule states that "a plaintiff can recover in tort only those economic losses resulting from injury to his person or damage to his property."[111] The purpose of the rule is to "to distinguish between those actions that are cognizable in tort and those that may be brought only in contract."[112] Where two contracting parties dispute whether one of the parties adequately performed, that dispute is one sounding in contract, not tort.

At least one case from this District has explicitly applied the rule to a negligence claim for a data breach where the parties were bound by a contract.

---

[110] *Huddle House, Inc. v. Two Views, Inc.*, 2013 U.S. Dist. LEXIS 48754 (N.D. Ga. Apr. 4, 2013); *GE v. Lowe's Home Ctrs., Inc.*, 279 Ga. 77, 78 (2005).
[111] *Id.*
[112] *City of Cairo v. Hightower Consulting Eng'rs, Inc.*, 278 Ga. App. 721, 728 (2006).

> The economic loss rule generally provides that a contracting party who suffers purely economic losses must seek his remedy in contract and not in tort [and that] a plaintiff can recover in tort only those economic losses resulting from injury to his person or damage to his property.[113]

The court noted that the rule was applied consistently in numerous jurisdictions.[114] LMT cannot overcome this bar to its negligence claim.

**2. LMT cannot show that Silverpop breached a duty owed to LMT.**

To establish negligence, a plaintiff must show that the defendant owed a duty to defendant and breached it.[115] Here, LMT alleges that Silverpop owed a duty of reasonable care to LMT.

LMT cannot establish this duty. In data security cases, courts have rejected a duty to utilize "commercially reasonable methods" to safeguard information.[116] "It is well-established that the occurrence of an unfortunate event is not sufficient to authorize an inference of negligence."[117] To prove negligence, LMT must establish a standard of care for data security and how Silverpop's conduct failed to meet it. It is insufficient to claim that the Breach occurred and, thus, Silverpop was negligent.

---

[113] *Willingham v. Global Payments, Inc.*, 2013 U.S. Dist. LEXIS 27764 (N.D. Ga. Feb. 5, 2013)(citing *City of Cairo*, 278 Ga. App. 721, 728 (2006)).
[114] *Id.* (citing *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 531 (N.D. Ill. 2011) and *In re Heartland Payment Sys., Inc., Customer Data Sec. Breach Litig.*, 834 F. Supp. 2d 566, 590 (S.D. Tex. 2011)).
[115] *Kraft Reinsurance Ir., Ltd. v. Pallets Acquisitions, LLC*, 845 F. Supp. 2d 1342, 1353 (N.D. Ga. 2011) (elements for a negligence).
[116] *See, e.g.*, *Willingham* at *64.
[117] *Id.* (citing *Johnson v. MARTA*, 230 Ga. App. 105, 106, (1998)).

LMT has not presented any evidence establishing an applicable standard of care. It relies exclusively on its expert, Roger Nebel to establish the relevant standard of care, but Nebel was unable to articulate any identifiable standard of care for data security or how Silverpop breached that standard. In his expert report, Nebel concludes that "Silverpop was extremely negligent because it failed to employ basic and well-established information security standards," but he fails to explain what that those "information security standards" are.[118] At one point in his report, Mr. Nebel vaguely refers to "Security Best Practices" but merely notes that these "vary by industry, focus, technical expert, contractual or legal definition, and the like."[119] But "best practices" does not establish a standard of care. [120] Nebel's deposition further establishes that there is not one uniform standard of care. He admits that "[t]oday there are dozens of standards, frameworks, methodologies, and the like."[121] He only notes "examples."[122] This testimony merely shows that there are a number of different practices used. Nebel fails to establish that any of his cited frameworks are ordinarily employed in Silverpop's industry under similar conditions to those faced by Silverpop. In fact, some of these so-called "standards" are plainly not applicable. Nebel cites the

[118] Deposition of Roger Nebel, Report at Ex.7, ¶16.
[119] Nebel Rep., ¶20.
[120] *See Somerville v. United States,* 2010 U.S. Dist. LEXIS 71969, *15 n.9 (M.D. Fla. June 30, 2010) ("The standard of care is not equivalent to 'best practices.'").
[121] Nebel Rep., ¶20.
[122] Nebel Rep., ¶20.

Gramm-Leach-Bliley Act, for example, which is, by definition, only applies to "financial institutions."[123] He admits it's not applicable to Silverpop.[124] Another example, Sarbanes-Oxley, is related to financial controls for publicly-traded companies.[125] Silverpop is not publicly-traded. When asked to describe what he means by "internet-facing enterprise best practices," Nebel points to "the wealth of information that has grown up in the 30 years or 40 years that information security has been a field of study in the world. It's just that body of knowledge, if you will."[126] Nebel's report contains claims concerning security protocols that Silverpop failed to implement, but without any industry standard of care against which to compare what Silverpop actually did. When directly asked "what specific controls do you believe Silverpop should have employed to detect illicit use of the Engage platform," Nebel responded, "I don't specifically state any."[127] Thus, Nebel's opinion does not support a negligence claims, and summary judgment is therefore appropriate.

## CONCLUSION

For the foregoing reasons, Plaintiff Silverpop is entitled to summary judgment.

[signatures on following page]

[123] 15 U.S.C. §§ 6801-6809.
[124] Nebel Dep., 199:12.
[125] 15 U.S.C. § 7262 (2006)).
[126] Nebel Dep., 26:13-17.
[127] Nebel Dep., 123:9.

Respectfully submitted this 13th day of August 2013.

**TROUTMAN SANDERS LLP**

*/s/ John P. Hutchins*
John P. Hutchins
Georgia Bar No. 380692
*john.hutchins@troutmansanders.com*
Courtney E. Ferrell
Georgia Bar No. 575948
*courtney.ferrell@troutmansanders.com*
Benjamin W. Cheesbro
Georgia Bar No. 648368
*benjamin.cheesbro@troutmansanders.com*

For Plaintiff Silverpop Systems, Inc.

5200 Bank of America Plaza
600 Peachtree Street, N.E.
Atlanta, GA 30308-2216
Telephone: (404) 885-3000
Facsimile: (404) 885-3900

**Certification of Counsel**

I hereby certify that this document is submitted in Times New Roman 14 point type as required by N.D. Ga. Local Rule 5.1(C).

*/s/ John P. Hutchins*
John P. Hutchins
Georgia Bar No. 380692